Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	MB Docket No. 02-230
Digital Broadcast Copy Protection	)	

REPLY COMMENTS OF VERIDIAN CORPORATION

Paul B. Schneck
Vice President and Chief Technology Officer
Veridian Corporation
1200 South Hayes Street, Ste. 1100
Arlington, VA 22202
(703) 575-3100

Pantelis Michalopoulos
Rhonda M. Bolton
Steptoe & Johnson LLP
1330 Connecticut Avenue NW
Washington, DC 20036
(202) 429-3000

Counsel for Veridian Corporation

February 21, 2003

SUMMARY

Veridian Corporation ("Veridian"), a provider of information technology solutions and engineering services to government agencies and the private sector, and developer of the VeriFIDES™ digital copy protection technology, requests that the Commission conduct on an expedited basis a negotiated rulemaking, whether formal under the Negotiated Rulemaking Act[1] or informal as done by other agencies. The Commission should convene a negotiated rulemaking committee and direct it to consider the following issues:

- The effectiveness (including a cost-benefit analysis) and appropriateness of the broadcast flag technology proposed by certain commenters in this proceeding;
- The effectiveness (including a cost-benefit analysis) and appropriateness of source-encryption-based technologies;
- The standards that must be satisfied by any accepted technology or implementation method, including the ability to adapt to and incorporate technological advances and the flexibility to respond to the evolving demands of consumers; and
- The interaction between the questions raised by the NPRM and digital copy protection for Multi-Channel Video Programming Distribution platforms.

A negotiated rulemaking is the best way forward in this proceeding. On the one hand, the comments confirm that the Commission should not prescribe the broadcast flag technology on the record assembled so far in this proceeding. On the other hand, the comments also confirm that there is a real problem that needs to be solved and a meaningful role for the Commission to assist industry in the effort to fashion a solution. In Veridian's view, that solution includes a choice among multiple source encryption methodologies that can be used to scramble components of ancillary digital broadcast services and that all satisfy certain standards

---

[1] *See* 5 U.S.C. § 561 *et seq.*

– minimum effectiveness and robustness, openness, mutual compatibility, respect for consumer privacy, and the like. In this way, standard-setting will pave the path for the market to be allowed to pick favored encryption methods, while at the same time these methods will satisfy certain public interest safeguards. Because private initiative alone has not proven successful with standard-setting in this area, the Commission can and should help by spearheading the effort. A negotiated rulemaking is the appropriate regulatory vehicle towards such a solution, consistent also with the views of commenters such as Motorola and Public Knowledge. *See, e.g.*, Comments of Motorola at 11 (suggesting that the rules established in the Federal Advisory Committee Act, 5 U.S.C., App. 2 (1996) be used as a model for a standard-setting body); Comments of Public Knowledge and Consumers Union ("Consumer Groups' Comments") at 2 (urging the Commission to initiate public and private fact-gathering processes before going forward with development and implementation of a rule).

Available evidence shows that the broadcast flag would be both costly and ineffective, and many commenters have raised valid questions about the Commission's authority to impose it in the first place. It is costly because it requires universal adoption. The comments of the Motion Picture Association of America ("MPAA") *et al.* make clear that all consumer digital television ("DTV") devices containing modulators and demodulators must incorporate the hardware needed to recognize the flag.[2] Indeed, these comments show that many more "downstream" devices, including personal computers, must either meet the same requirements or be disqualified from access to digital broadcast content. This means one of two things: either the implementation cost for the broadcast flag will be higher still or, as the consumer organizations correctly point out, adoption of the flag would frustrate the long-sought goal of

[2] *See* MPAA Comments, Attachment A ("White Paper: A Proposal for Protection of Unencrypted Digital Broadcast Television" (Dec. 6, 2002)), at 4-5.

convergence between the PC and the television set, at significant expense to the consumer.[3] Furthermore, in addition to entailing significant implementation costs, the universal character of the broadcast flag also casts significant doubt on the Commission's jurisdiction to prescribe it.

For all its costs, the benefits of the broadcast flag are shown on this record to be illusory. Specifically, many opponents of the technology point out, and no proponent appears to dispute, that the technology is only as good as its weakest link. Any digital box not equipped with the required hardware will be able to receive the digital broadcast signal without any copy protection being afforded to that signal. Unless the Commission's universal adoption requirement succeeds universally, the broadcast flag will likely not achieve its stated goal and would leave content providers as reluctant to license their content as before.

Based on this cost and benefit analysis, it would be highly questionable whether adoption of the broadcast flag would be justified even if it were the only methodology that could induce the digital broadcast of currently withheld digital content. In fact, however, this is not the case. Source encryption offers a solution that is less costly, more effective, and can be more narrowly tailored to the problem of safeguarding broadcasts of premium content. Moreover, the Commission has much more solidly based authority to require source encryption for certain kinds of services (ancillary and supplementary services) than it has to impose a universal methodology for receiving all digital broadcasts.

Source encryption is less costly exactly because it need not be universally implemented. If, for example, protecting ancillary and supplementary services is what it takes to

---

[3] While the content providers are correct in stating that not all content need be protected from copying, this makes a universal mandate for all receive devices overbroad and even less justified.

fix the problem of holding back premium content,[4] the cost implications of an encryption-based solution are limited to the receive equipment of those consumers interested in receiving the services in question. All other consumers could still use devices that do not incorporate a decryption chip.

At this lower cost, encryption would bring about greater benefit: no one disputes that encryption would afford greater copy protection than a broadcast flag solution. Among other things, the existence of "non-compliant" devices would not in the least diminish the protection offered by these technologies, as these devices would simply be unable to unscramble encrypted content even as they could receive all other broadcast services. Encryption would also be more flexible in offering exactly as much copy protection as the market demands or as law allows. By contrast, the broadcast flag is a blunt instrument that, in the instances where it works, will prohibit all but local digital copying, i.e., such copies would only be usable on the network wherein they were produced. Consumers would lose the ability to 'space shift' content, e.g., to take a copy from one's home to one's office for viewing. It is therefore a serious misperception to view the broadcast flag as a "light," and more palatable, method of copy protection. In fact, the reverse is the case. Source encryption is far less intrusive than the flag, both because the flag affects all DTV consumers, and because it precludes more copying of flagged content than necessary or desirable. Moreover, with source encryption methods, new and potentially improved technologies can still enter the marketplace – something that is not possible with the broadcast flag.

---

[4] *See, e.g.*, MPAA Comments at 14 (predicting that some content providers would decide not to protect their material, while "high-value programming including films and first run series" would generally be protected).

This does not mean that continuing Commission engagement is unnecessary, however. Veridian believes that market forces should be allowed to choose among many different digital copy protection methodologies, but the divergence of views presented in this proceeding makes it clear that standard-setting is necessary for the market to be allowed to work, for the public interest in DTV transition to be served, and for consumers' rights (e.g., fair use, privacy) to remain intact. The Commission clearly has the power to help in the process and to conduct a negotiated rulemaking on these issues. Veridian hereby offers its views on the standards that the Commission can and should consider to facilitate a market-based solution.

TABLE OF CONTENTS

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	MB Docket No. 02-230
Digital Broadcast Copy Protection	)	
	)	

REPLY COMMENTS OF VERIDIAN CORPORATION

Veridian Corporation ("Veridian"), a provider of information technology solutions and engineering services to government agencies and the private sector, and developer of the VeriFIDES™ digital copy protection technology, hereby submits the following reply comments in response to the comments filed in the above-captioned proceeding.[1]

I. INTRODUCTION

Veridian requests that the Commission conduct on an expedited basis a negotiated rulemaking, whether formal under the Negotiated Rulemaking Act[2] or informal as done by other agencies. The Commission should mandate the negotiated rulemaking committee to consider the following issues:

- The effectiveness (including a cost-benefit analysis) and appropriateness of the broadcast flag technology proposed by certain commenters in this proceeding;

---

[1] *In the Matter of Digital Broadcast Copy Protection*, Notice of Proposed Rulemaking, MB Docket No. 02-230 (rel. Aug. 9, 2002) ("NPRM").

[2] *See* 5 U.S.C. § 561 *et seq.*

- The effectiveness (including a cost-benefit analysis) and appropriateness of source-encryption-based technologies;
- The standards that must be satisfied by any accepted technology or implementation method, including the ability to adapt to and incorporate technological advances and the flexibility to respond to the evolving demands of consumers; and
- The interaction between the questions raised by the NPRM and digital copy protection for Multi-Channel Video Programming Distribution ("MVPD") platforms.

A negotiated rulemaking is the best way forward in this proceeding. On the one hand, the comments confirm that the Commission should not prescribe the broadcast flag technology on the record assembled so far in this proceeding. On the other hand, the comments also confirm that there is a real problem that needs to be solved and a meaningful role for the Commission to assist industry in the effort to fashion a solution. In Veridian's view, that solution includes a choice among multiple source encryption methodologies that can be used to scramble components of ancillary digital broadcast services and that all satisfy certain standards – minimum effectiveness and robustness, openness, mutual compatibility, respect for consumer privacy, and the like. In this way, standard-setting will pave the path for the market to be allowed to pick favored encryption methods, while at the same time these methods will satisfy certain public interest safeguards. Because private initiative alone has not proven successful with standard-setting in this area, the Commission can and should help by spearheading the effort. A negotiated rulemaking is the appropriate regulatory vehicle towards such a solution, consistent also with the views of commenters such as Motorola and Public Knowledge. *See, e.g.*, Comments of Motorola at 11 (suggesting that the rules established in the Federal Advisory Committee Act, 5 U.S.C., App. 2 (1996) be used as a model for a standard-setting body); Comments of Public Knowledge and Consumers Union ("Consumer Groups' Comments") at 2

(urging the Commission to initiate public and private fact-gathering processes before going forward with development and implementation of a rule).

Veridian hereby offers its views on the standards that the Commission can and should consider to facilitate a market-based solution.

II. THE COMMISSION SHOULD NOT REQUIRE A BROADCAST FLAG ON THE RECORD OF THIS PROCEEDING

Even at this early stage of the Commission's consideration of the broadcast flag proposal, the record compiled thus far demonstrates that the broadcast flag is both costly and ineffective. The Commission, therefore, should not mandate use of the broadcast flag.

A. Adoption Of The Flag Is Costly

The broadcast flag technology is costly because it must be adopted universally to work. Devices that do not recognize the flag would enable circumvention of the flag. The universal adoption requirement is reflected in the Motion Picture Association of America ("MPAA") *et al.*'s broadcast flag proposal. MPAA's comments state that "in order for the Broadcast Flag Solution to be complete," the flag must be incorporated into all devices capable of demodulating or modulating the DTV signal. *See* MPAA Comments, Attachment A ("Whitepaper: A Proposal for Protection of Unencrypted Digital Broadcast Television" (Dec. 6, 2002), at 4). To start, this would mean *all* television sets would have to incorporate circuitry capable of responding to the broadcast flag. Consumers may not react positively to such a requirement, especially coming on the heels of another universal implementation requirement, the mandate that all new television sets, VCRs, and DVD players/recorders have digital tuners by July 1, 2007. *See In the Matter of Review of the Commission's Rules and Policies Affecting the*

Conversion to Digital Television, Second Report and Order and Second Memorandum Opinion and Order, MM Docket No. 00-39, FCC 02-230 (rel. Aug. 9, 2002).

Another commenter has recognized that the flag would be costly in another way as well. Thomson, Inc. explains that incorporation of the broadcast flag at the point of demodulation, as proposed by MPAA, would require that demodulators have a demultiplexer and a microprocessor on a single integrated circuit, and that a circuit with these characteristics does not exist today. *See* Comments of Thomson, Inc. at 16-17. Veridian agrees with Thomson that in the absence of a non-discrimination requirement, such a circuit could only be offered by the two companies that have the intellectual property rights for all of these technologies, and reliance on technology controlled by only two companies can lead to competitive concerns and ultimately, higher hardware costs for consumers. *See id.* [3]

While the MPAA tries to present the universal implementation requirement as limited, its own proposal shows otherwise. MPAA's comments make clear that the broadcast flag must be incorporated into many other types of downstream devices, such as personal computers ("PCs"), in order for those devices to access digital broadcast content. *See* MPAA Comments at 16-17 (asking the Commission to mandate that "downstream products" may not access digital broadcast content unless they comply with the broadcast flag regime and their manufacturers have "filed a 'written commitment'" to incorporate broadcast flag technology). *See id.* at 17. MPAA makes no effort to describe the types of downstream devices affected by its proposal beyond mentioning computers and "IT" products, perhaps because the affected products

[3] In contrast, Veridian, in submissions to the Consumer Electronics Association, the World Airline Entertainment Association, and the Society of Motion Picture and Television Engineers, has offered to license its source encryption technology on reasonable and non-discriminatory terms. As explained below, Veridian believes that this should be requested of any acceptable digital copy protection method.

are too numerous to count. MPAA attempts to assume away the tremendous cost associated with incorporating broadcast flag technology in such a wide range of products by suggesting that "the vast majority of products will be designed either not to access digital broadcast television content at all in usable form," or to access it only after it has been passed from a regulated product via a protected output, *see id.* at 4. This does not diminish the extent of the problem, however. It means only that CE manufacturers and consumers alike are faced either with the Scylla of higher costs or the Charybdis of insulated television and PC equipment that are prohibited from talking to one another by regulatory fiat. *See* Consumer Groups' Comments at 2-5. This latter result is directly contrary to Commission policies in favor of promoting convergence between telecommunications equipment and the personal computer.[4] Indeed, MPAA itself acknowledges that consumers will likely desire the ability to access content utilizing a wide variety of devices. *See* MPAA Comments at 3 (declaring that the definition of "personal digital network environment" should be flexible).

And the costs of universal implementation would be even higher if another category of content owners, those with ownership interests in music, demand that the technology be incorporated in devices capable of manipulating DTV audio, such as stereo systems with CD burners. *See, e.g.*, Comments of The National Music Publishers' Association at 9 (pointing out that there is a "risk to copyrights in areas beyond the narrow field of DTV broadcast").

---

[4] *See, e.g.*, *In the Matter of Advanced Television Systems and Their Impact Upon the Existing Television Broadcast Service*, 11 FCC Rcd. 17771, 17789 (1996), ¶ 39 (observing that the DTV standards adopted by the Commission will promote interoperability and convergence of computer equipment and television).

B. The Benefits From The Flag Are Illusory

For all its costs, this record shows that the benefits of the broadcast flag are illusory. As many commenters recognize, the broadcast flag technology can be circumvented by any device not incorporating the technology, whether they be legacy devices or ones built or modified by pirates. *See, e.g.*, Comments of Motorola at 4 (the broadcast flag as currently defined, is "an ineffective security technology"); Comments of Public Knowledge and Consumers Union (transmitting content "in the clear" as the broadcast flag proposal suggests "leaves the front door open"); Comments of the Electronic Frontier Foundation at 7-8 (the broadcast flag is "an absurdly weak form of security technology"). Thus, unless the universal adoption requirement succeeds universally, which is very doubtful, the broadcast flag is likely to leave content providers as reluctant to license their content as before. None of the broadcast flag proponents appears to dispute the weakness of the technology, and some even acknowledge its inferiority to source encryption. *See* Comments of Digital Transmission Licensing Administrator LLC at 7 ("[f]rom a technical perspective, protection is most effective when applied at the source, such as distribution of content in an encrypted form," describing content protection at the point of demodulation (the broadcast flag scheme), in contrast, as the "next most effective means"); *see also* remarks by Andy Setos, President of Engineering, Fox Entertainment Corp., at the "Battle Over the Broadcast Flag: The IP Wars and the HDTV Transition" CATO Institute Policy Forum (Feb. 5, 2003) (*available at* http://www/cato.org/events/030205pf.html), at time index 47:32 ("Characterizing the flag as it will only do a, very little, ahh, yes you are right if nothing else happens, we need to have more success at managing legacy technologies. . . . Alone it [the broadcast flag] doesn't really ring any bells, because there are so many work arounds.").

Therefore, its high cost aside, the broadcast flag would not be effective in solving the problem of content providers holding back premium content, and should not be adopted on this record.

C. The Commission's Jurisdiction Is Doubtful

In addition to requiring significant implementation costs for illusory protection, there is doubt whether the Commission has the authority to prescribe universal adoption of the broadcast flag. As discussed above, circuitry recognizing the broadcast flag must be universally incorporated in hardware devices for the system to work at all. Yet, contrary to the arguments of some commenters, it is not clear that the Communications Act gives the Commission authority to require that consumer electronics and other devices respond to the flag.

First, nowhere does the Communications Act explicitly grant such authority. Section 336 explicitly authorizes the Commission to regulate DTV in only two areas: DTV license eligibility, *see* 47 U.S.C. § 336(a)(1)[5], and the provision of "ancillary or supplementary services" by DTV licensees, *see* 47 U.S.C. § 336(a)(2). The Commission has in turn explained that ancillary or supplementary services "include, but are not limited to, computer software distribution, data transmissions, teletext, interactive materials, aural messages, paging services, audio signals, [or] subscription video." *See In the Matter of Fees for Ancillary or Supplementary Use of Digital Television Spectrum Pursuant to Section 336(e)(1) of the Telecommunications Act of 1996*, 14 FCC Rcd. 3259, 3270 (1998) ("*DTV Fees R&O*"), ¶ 31 (quoting 47 C.F.R. §73.624(c)) (internal quotation marks omitted).

---

[5] Section 336(a)(1) instructs the Commission to "limit the initial eligibility for such licenses to persons that, as of the date of such issuance, are licensed to operate a television broadcast station or hold a permit to construct such station (or both)."

The MPAA maintains that Section 336 of the Communications Act grants the Commission explicit authority to mandate a broadcast flag regime, but MPAA misreads the statute. *See* MPAA Comments at 29-32. Specifically, the MPAA claims that explicit authority to mandate the broadcast flag is provided in Sections 336(b)(4) and (5). Section 336(b)(4) states that the FCC shall "adopt such technical and other requirements as may be necessary or appropriate to assure the quality of the signal used to provide advanced television services, and may adopt regulations that stipulate the minimum number of hours per day that such signal must be transmitted." Section 336(b)(5) allows the Commission to "prescribe such other regulations as may be necessary for the protection of the public interest, convenience, and necessity."

These provisions, however, pertain only to regulations "that allow the holders of [advanced television services] licenses to offer such ancillary or supplementary services on designated frequencies as may be consistent with the public interest, convenience, and necessity." *See* 47 U.S.C. § 336(a)(2). Congress has made this clear by prefacing the entire Section § 336(b) with the sentence: "In prescribing *the regulations required by subsection (a) of this section*, the Commission shall – . . . ." 47 U.S.C. § 336(b) (emphasis added). In turn, the only "regulations required by subsection (a)" are those relating to ancillary or supplementary services. *See* 47 U.S.C. § 336(a)(2). As the Commission itself has put it in its Report and Order prescribing fees for ancillary and supplemental use of DTV spectrum: "Congress also gave the Commission discretion to prescribe such other regulations *with respect to ancillary or supplemental services* 'as may be necessary for the protection of the public interest, convenience or necessity.'" *DTV Fees R&O*, 14 FCC Rcd. at 3259, ¶ 2 (citing Section 336(b)(5)) (emphasis added). The broadcast flag, however, is not such a narrowly tailored requirement at all. To the contrary, the flag would affect the receipt of all digital broadcast services, not only ancillary or

supplementary offerings. It follows that, contrary to the MPAA's allegation, the provisions of Section 336(b) cannot be a source of authority to prescribe the flag.

Next, some commenters argue that implicit authority to regulate hardware devices in this manner can be derived from provisions of Title I and Title III of the Communications Act granting the Commission authority over matters reasonably ancillary to its jurisdiction under those titles. *See* MPAA Comments at 32-41. While Veridian does not take a position on this question, it is certainly not clear that such implicit authority would be broad enough to encompass a universal prescription affecting the receipt by consumers of any and all digital broadcast services.

According to MPAA, there are two sources of Commission authority over matters reasonably ancillary to its jurisdiction: first, Section 4(i) of the Act, which states that the Commission "may perform any and all acts, make such rules and regulations, and issue such orders, not inconsistent with this chapter, as may be necessary in the execution of its functions," 47 U.S.C. § 154(i); and second, Section 303(r) within Title III, which similarly provides that in the broadcast context, the Commission may "make such rules and regulations and prescribe such restrictions and conditions, not inconsistent with law, as may be necessary to carry out the provisions of this chapter. . . ." 47 U.S.C. § 303(r). Neither provision, however, supports unequivocally the Commission's authority to do something as broad as requested by MPAA -- *universally* prescribe *one* digital copy protection methodology for the receipt of *all* digital broadcast services.

The Commission long ago recognized that Title I does not confer "plenary authority over 'any and all enterprises which happen to be connected with one of the many aspects of communications.'" *U.S. v. Southwestern Cable Co.*, 392 U.S. 157, 164 (1968) (citing

CATV and TV Repeater Services, 26 F.C.C. 403, 429 (1959)). The D.C. Circuit recently opined on the breadth of the Commission's ancillary authority under Section 4(i) in striking down the Commission's rules requiring video description of television programming, a service for the visually impaired that involves aural descriptions of a television program's key visual elements. The Commission had argued that it derived jurisdiction to mandate video description partly from Section 4(i). The court rejected this assertion out-of-hand, explaining that Section 4(i) standing alone grants no authority to the Commission to act. Rather, Section 4(i) only authorizes regulation where necessary to carry out another, express statutory directive. *MPAA v. FCC*, 309 F.3d 796 (D.C. Cir. 2002). The court fully endorsed Chairman Powell's dissent from the Video Description Report and Order, which stated:

> It is important to emphasize that Section 4(i) is not a stand-alone basis of authority and cannot be read in isolation. It is more akin to a 'necessary and proper' clause. Section 4(i)'s authority must be 'reasonably ancillary' to other express provisions. And by its express terms, our exercise of that authority cannot be 'inconsistent' with other provisions of the Act. The reason for these limitations is plain: Were an agency afforded *carte blanche* under such a broad provision, irrespective of subsequent congressional acts that did not squarely prohibit action, it would be able to expand greatly its regulatory reach.

Id. at 806 (quoting *Implementation of Video Description of Video Programming*, Report and Order, 15 FCC Rcd. 15230, 15276 (2000) (Powell, dissenting)).

Nor is it clear that a statutory grant of authority can be found in a combination of Title I and the Commission's authority to regulate television broadcasting. MPAA claims that the broadcast flag will "protect[] the integrity of digital broadcast transmissions," which "relates directly to broadcasting and therefore falls squarely within the Commission's jurisdiction," MPAA Comments at 36. However, this may be a somewhat attenuated link.

The other provision cited by the MPAA as conferring implicit jurisdiction to require broadcast flag circuitry in receivers and other hardware, Section 303(r), is likewise a questionable source of such authority. Section 303(r) permits the Commission to regulate in the public interest "as may be necessary to carry out the provisions of [the] Act." However, as the D.C. Circuit has explained, "the FCC cannot act in the 'public interest' if the agency does not otherwise have the authority to promulgate the regulations at issue. *** "The FCC must act pursuant to *delegated authority* before any 'public interest' inquiry is made under § 303(r)." *MPAA*, 309 F.3d at 806 (emphasis in original).

In sum, the Commission may have the authority to prescribe the broadcast flag, but this is far from certain. In light of this uncertainty, the Commission should at a minimum be reluctant to embark on a regime of complex regulation that may be reversed or remanded by the courts on purely jurisdictional grounds alone. The Commission should do so only if the benefits are so certain and concrete as to outweigh both the costs and the jurisdictional uncertainty. On the record assembled so far in this proceeding, this has not been established.

III. SOURCE ENCRYPTION IS A BETTER SOLUTION

The flaws of the broadcast flag do not mean that the Commission should do nothing. In Veridian's view, one problem hampering DTV transition identified by the Commission and by many commenters, does exist and is an acute one: copyright holders are reluctant to permit the distribution of high-value, e.g., high definition programming without the safeguard of digital copy protection.[6] Source encryption is less costly while being an effective

[6] While Veridian does not disagree with Public Knowledge that rigorous evidence of the problem is also missing from the record, further proceedings will accommodate the consumer organizations' call for such evidence. This is exactly consistent with the view expressed by Public Knowledge and Consumers Union. *See* Consumer Groups' Comments at 2-3.

solution to the problem. In addition, source encryption is a more flexible digital copy protection regime compared to the blunt protection offered by the broadcast flag, and rules governing source encryption are more clearly within the Commission's authority than would be the prescription of a broadcast flag requirement.

The Commission does not need to, and should not, prescribe one encryption methodology over others, but the Commission's role remains meaningful and necessary. The Commission should help with standard setting that will allow a multiplicity of methods based upon source encryption to vie for acceptance and market forces to pick and shape the ones that are most suitable. And, the Commission should consider criteria that each of these methods should satisfy to ensure that the public interest in the DTV transition is served and that consumer rights are respected.

A. The Costs Of Source Encryption Are Lower Than Those Of The Broadcast Flag, While Its Benefits Are Greater

Even a rudimentary cost-benefit analysis will reveal that source encryption is clearly a better copy protection solution than the broadcast flag. First, source encryption will be less costly overall than the broadcast flag regime simply because it is a solution more narrowly tailored to the extent of the problem – protecting premium content that would be held back without protection. Veridian specifically believes that protecting premium services will go a long way towards solving that problem. Several commenters, including the content providers themselves, acknowledge that not all content need be protected.[7] Unlike the broadcast flag, therefore, source encryption technology need only be incorporated into receive devices of a

[7] *See, e.g.*, MPAA Comments at 14 (predicting that some content providers would decide not to protect their material, while "high-value programming including films and first run series" would generally be protected). *See also* Comments of Motorola at 7 (observing the same).

subset of consumers – those interested in receiving premium content. All other consumers will not need to purchase receive devices that incorporate a decryption chip.

While source decryption will need to be incorporated in a small subset of receive equipment, even on a per unit basis the cost of incorporating a decryption chip in a single device is expected to be comparable to the hardware needed to recognize the broadcast flag. Also, unlike the broadcast flag, recording and playback devices need not incorporate any protection circuitry. Such circuitry is needed only in terminal viewing and display devices, e.g., DTV receivers. Veridian is not alone in recognizing the advantages associated with the narrowly tailored character of source encryption. *See, e.g.*, Comments of Motorola at 6-7.

As Thomson explains, however, the broadcast flag system proposed by MPAA would require that demodulators have a demultiplexer and a microprocessor on a single integrated circuit, and a circuit with these characteristics does not exist today. *See* Comments of Thomson, Inc. at 16-17. The circuitry required for the broadcast flag would therefore have to be developed and then, as noted above, incorporated into each and every device that *might* receive protected content.

The combination of narrower deployment and comparable per unit cost will translate into significantly lower overall cost for source encryption methodologies compared to the broadcast flag. At a lower cost, source encryption will deliver larger benefits, precisely because even without universal deployment it is not compromised – the Achilles heel of the broadcast flag regime. In contrast with that regime, devices that do not incorporate the chip do not affect the integrity of the copy protection afforded by the system. Such devices are simply incapable of reading the encrypted content. A cost/benefit comparison of the broadcast flag and

source encryption shows that it would be wrong for the Commission to prescribe a methodology that is both costlier and less beneficial, and certainly not now, on the record of this proceeding.

To the extent that any commenter may be opposed to source encryption due to concern that it is more costly to incorporate in individual consumer electronics devices, Veridian wishes to point out that there is no empirical evidence that broadcast flag circuitry is cheaper to implement, and, indeed, this appears unlikely. Of the major components of VeriFIDES™ that would be incorporated in hardware devices for example, the "encryption component" and the memory to hold the necessary software are items of trivial cost; and the processing software itself represents a non-recurring cost that can be spread out over all devices produced. Although any system to protect content must contain a protection component necessary for thwarting efforts to break into the hardware, VeriFIDES™, at nominal cost, can provide this protection by erasing the electronic secret (key) contained in the hardware device. VeriFIDES™ thus affords a higher level of protection than available in the static circuitry used by the broadcast flag, and most likely does so at a lower cost than the static circuitry necessary to provide similar protection to a broadcast flag system. At a minimum, therefore, the record in this proceeding is too underdeveloped to support opposition to source encryption on the basis of cost.

B. Source Encryption Affords Greater Flexibility And Is Better Able To Respect Fair Use Requirements And Accommodate The Public Interest

The broadcast flag compares to source encryption the way a meat cleaver compares to a scalpel. Whereas the broadcast flag, if it works, would prohibit any and all space shifting by consumers except within the same network, source encryption offers as much or as little copy protection as the market demands or the law allows. The flexibility of source encryption is well demonstrated by VeriFIDES™ technology, which allows copying, but requires each user to obtain a "ticket" to view protected content. The broadcast flag, moreover,

allows no situational parameters to control whether or not copying is permitted. In contrast, content owners, each using a VeriFIDES™ ticket, can do far more than direct whether or not copying would be allowed. Other parameters can be set as well, including, for example, start and end viewing dates, resolution (e.g., high definition, standard definition), maximum screen size, and premium services such as multi-channel sound, advance preview, or other (including future) enhancements. It follows that content providers and consumers can take advantage of a very broad range of options for access to protected material.

Several commenters have raised serious concerns regarding the implications for fair use of a copy protection regime. Logically, source encryption, which gives consumers and content owners a range of content protection options rather than only two, will be a more useful tool for market participants as the balance between intellectual property rights and fair use is struck.

Another apparent misconception about source encryption is that a regulatory impediment will prohibit source encryption of broadcast DTV signals. Indeed, it appears that the broadcast flag was developed by parties laboring under the impression that source encryption was not a permissible alternative for protecting DTV broadcasts. *See, e.g.*, Comments of The IT Coalition at 16-17 (describing rejection of the computer industry's source encryption proposal by the Broadcast Protection Discussion Group responsible for developing the flag proposal); Comments of the Digital Transmission Licensing Administrator, LLC at 7 (acknowledging that source encryption is the most effective method of content protection, but supporting the broadcast flag as the "next most effective means.")

The Commission, however, has not unequivocally foreclosed source encryption as an option for digital broadcasting, and certainly source encryption should be viewed as perfectly

acceptable at least for ancillary and supplementary services. This issue was broached by commenters in the rulemaking considering compatibility between cable systems and consumer electronics devices, and rather than summarily reject the suggestion, the Commission concluded that the record in that proceeding was not sufficient to allow the Commission to reach a conclusion as to whether encryption of digital over-the-air broadcast signals should be allowed. *See In the Matter of Compatibility Between Cable Systems and Consumer Electronics Equipment*, 15 FCC Rcd. 17568 (2000), at ¶¶ 31-32. The Commission has left this issue open to debate, and rightfully so. The current nominal restriction on encryption or scrambling of over-the-air broadcast programming exists only to effect the Commission's policy of preserving free-over-the air programming. *See In the Matter of Subscription Video*, 2 FCC Rcd. 1001, 1006 (1987). To the extent encryption is compatible with transmission of free over-the-air programming, as VeriFIDES™ encryption technology is,[8] the Commission's concern regarding loss of free over-the-air programming is not implicated.

Equally important, the Commission has recognized that ancillary and supplementary services can include subscription services, and a prohibition on source encryption would be completely inconsistent with that recognition. At least with respect to such services, therefore, source encryption is certainly an appropriate digital copy protection method. As it happens, of course, it is primarily the premium content included in such services that would most likely be held back without protection, meaning that digital copy protection may only be needed for such services anyway. The Commission should not settle for a method that even its

[8] As discussed above, should material be transmitted without copy protection (i.e., without using the optional source encryption), which may be the case for free over-the-air broadcasts if regulators or content owners decide to do so, source encryption systems will not prevent viewers from receiving this content even if the viewer has not purchased decryption equipment.

proponents appear to view as "second best," particularly where "second best" may not be effective at all.

C. In Contrast With The Broadcast Flag Adoption, Rules Governing Source Encryption Are Unquestionably Within The Commission's Jurisdiction

While it is not at all clear that the Commission has authority to mandate use of the broadcast flag, the Commission need not grapple with this uncertainty when it is far more clear that rules facilitating the deployment of source encryption are within the Commission's jurisdiction.

As explained above, Section 336 contains an express delegation of authority directing the Commission to promulgate technical requirements related to the provision of "ancillary or supplementary services." If the Commission were to determine that the problem of holding back certain premium content could and should be solved narrowly, i.e. by protecting the content that is most in need of protection, then there is absolutely no doubt that the Commission's involvement in source encryption standard setting will be well within the mandate of Section 336(b). Thus, the Commission may not need to tackle the more difficult jurisdictional questions associated with the scope of Title I or Section 303.

Moreover, in contrast with the broadcast flag proposal, the Commission's role need not and should not extend to prescribing a single methodology – a proposition that raises thornier jurisdictional questions by its sheer prescriptive nature and is certainly questionable as a policy matter, since it involves "picking a winner." Rather, the Commission's appropriate role is one of adopting standards that each of several methods will be capable of satisfying. This kind of rulemaking is no different than, for example, the Commission's standard-setting functions in the proceeding to develop service rules for new third generation (also known as "3G") wireless systems, where the Commission is involved in the standard-setting process even as it refrains

from getting into the business of "picking a winner" among various technologies that could be used to deliver 3G services. *See In the Matter of Service Rules for Advanced Wireless Services in the 1.7 GHz and 2.1 GHz Bands*, Notice of Proposed Rulemaking, WT Docket No. 02-353, FCC 02-305 (rel. Nov. 22, 2003), ¶ 4 (explaining the Commission's plan to allow 3G licensees "greater freedom to determine the specific technologies to be used and services to be offered" while the Commission sets standards for critical matters such as prevention of interference).

IV. A COMMISSION-ASSISTED STANDARD-SETTING PROCESS IS NECESSARY

Veridian believes that market forces should be allowed to choose among many different source encryption methodologies, but the divergence of views presented so far in this proceeding makes it clear that standard-setting is necessary for the market to be allowed to work, for the public interest in the DTV transition to be served, and for consumers' rights (e.g., fair use and privacy) to remain intact. As noted above, the Commission clearly has the power under Title I and Title III of the Communications Act to assist in the process of developing a source encryption-based copy protection regime. Veridian hereby offers its views on the standards that the Commission can and should consider to facilitate a market-based solution.

A. Standards Are Necessary To Allow The Market To Work, Facilitate DTV Transition By Ensuring Over-The-Air Availability Of Premium Content, And Ensure Respect For Consumers' Rights

While the private Broadcast Protection Discussion Group ("BPDG") began the process of attempting to reach consensus on a copy protection system, many commenters do not agree that the BPDG's broadcast flag proposal is an appropriate solution. *See, e.g.*, Comments of the IT Coalition at 15-19; Comments of Motorola at 4-5; Comments of the Electronic Frontier Foundation at 7-8. Of particular concern are questions concerning the propriety of Commission reliance on the findings of BPDG, a group that was "expressly limited in its mission." *See*

Consumer Groups' Comments at App. A, p. 2; *see also, e.g.*, Comments of the IT Coalition at 23; Comments of the Information Technology Association of America at 8-11. Moreover, there is not complete accord as to whether the record so far adequately demonstrates need for DTV copy protection at all. *See, e.g.*, Consumer Groups' Comments at 3-11; Comments of Electronic Frontier Foundation at 3-5; Comments of Philips Electronics North America Corp. at 2, 7. And a diverse group of commenters, including hundreds of individual consumers, have expressed concern about whether a copy protection system can be mandated consistent with consumers' right to fair use of content under copyright law. *See, e.g.*, Comments of Philips Electronics North America Corp. at 19; Comments of the Information Technology Association of America at 15; Consumer Groups' Comments, App. A at 3-4; Comments of John Collier, Silicon Graphics, Inc.

The divergence of views on these important topics among participants with widely varied interests calls out for Commission involvement in setting standards. The private process has failed thus far. Disagreement as to technical matters has prevented the market from working in this regard. Commission involvement at this stage can facilitate development of standards that will allow the market to work toward developing an acceptable technology capable of serving the public interest in the DTV transition. Standards must also be set to help achieve balance between consumer interests and the desires of the content community.

A number of commenters support a neutral approach to developing a copy protection system, allowing the market to select the most suitable method for protecting DTV transmissions. *See, e.g.*, Comments of TiVo, Inc. at 7-8; Comments of The Information Technology Association of America at 9-12. To this end, any Commission regulation in this area should be limited to the adoption of standards that must be met by any copy protection

system ultimately adopted to ensure that the system will serve its intended purpose. Veridian believes that appropriate standards must include:

- Minimum standards of robustness and reliability. The minimum standard should include, for example, no "shared secrets," as such technology is apt to fail;
- Openness. The encryption and protection method must be open to all consumer equipment manufacturers, distribution platforms, and all content providers indiscriminately;
- Visibility. The algorithms, specifications, and parameters of the method must be open to consumers so that they may ensure themselves that their interests in fair use and privacy are met. Importantly, the efficacy of the system should not be compromised by such visibility;
- Renewability. In the event of compromise, the system must provide a means to protect future content – without a total recall or invalidation of all installed consumer equipment;
- Compatibility. The method must not preclude use of a different, competing method, and must allow next-generation techniques to be deployed with minimal conversion requirements;
- Simplicity. The Commission might consider limits to the complexity of the protection language that can be deployed. Such limits could in turn contain the cost of the copy protection hardware that needs to be incorporated in consumer equipment;
- Privacy. A technology must protect consumer privacy and anonymity if consumers desire.

Technologies that comply with these minimum standards will serve the aims of providing reliable protection to content, while minimizing costs to consumers and preserving their rights.

B. A Negotiated Rulemaking Is The Appropriate Step Forward

The Negotiated Rulemaking Act allows federal agencies to formally convene an advisory committee to attempt to reach a consensus on a proposed rule. *See* 5 U.S.C. § 561 *et*

seq. Establishment of a formal "negotiated rulemaking committee" must be done in accordance with the Federal Advisory Committee Act, Pub. L. 92-463, § 1, 86 Stat. 770 (Oct. 6, 1972) (*codified at* 5 U.S.C. Appendix 2, § 1), and may occur only after the agency makes a determination that a negotiated rulemaking would be in the public interest based on criteria set forth in the Negotiated Rulemaking Act, and the agency publishes a notice in the Federal Register indicating its intent to establish a negotiated rulemaking committee. *See* 5 U.S.C. §§ 563, 564. The committee's operations must comply with the Federal Advisory Committee Act which requires, among other things, that the committee meet publicly, make all of its records publicly available, and meet only in the presence of an agency officer or employee. *See* 5 U.S.C. App. 2, § 10.

By enacting the Negotiated Rulemaking Act, Congress expressed its agreement with the observation of several administrative law scholars that negotiated rulemaking offers a number of advantages over more typical notice-and-comment procedures in certain types of situations. For example, some observers have explained that negotiated rulemaking can lead to speedier regulatory resolutions where the matter at issue is a "new topic," where the agency is considering standards for a particular industry, and where issues have been sufficiently crystallized to make an exchange useful but positions have not become hardened and large investments have not yet been made. *See generally* 1 Charles Koch, Administrative Law Treatise § 4.36; Phillip Harter, *Negotiating Regulations: A Cure for Malaise*, 71 Geo. L.J. 1 (1982). The DTV copy protection issue fits the foregoing profile perfectly: the issue is relatively "new," and standards are the matter under consideration. The fact that many commenters agree that some type of copy protection will be necessary means that at least this issue has been sufficiently crystallized to make useful an exchange regarding what method of

protection will be most appropriate. In addition, at this early stage, the participants' positions do not appear to be "hardened," which is not surprising given that large investments have not yet been made in any particular technology as a result of regulatory mandates.

Negotiated rulemaking procedures have been used successfully by a number of agencies, including the Commission. In the proceeding for licensing "little-LEO" Mobile Satellite Service users, for example, the Commission adopted rules to govern the licensing and regulation of the service and observed that the generally uniform support of the ultimate rule was "due in large part to the cooperation of those affected parties who assisted the Commission in the development of regulations through the negotiated rulemaking process." *In the Matter of Amendment of the Commission's Rules to Establish Rules and Policies Pertaining to a Non-Voice, Non-Geostationary Mobile-Satellite Service*, 8 FCC Rcd. 8450 (1993) at ¶ 2. As the Commission further explained, "[t]he parties' willingness to participate in the Commission's initial negotiated rulemaking process . . . has greatly assisted the Commission staff and has streamlined this rulemaking process."). *Id. See also In the Matter of Access to Telecommunications Equipment and Services by Persons With Disabilities*, 11 FCC Rcd. 8249 (1996) at ¶ 5 (the Commission convened a "Hearing Aid Compatibility Negotiated Rulemaking Committee" to consider the fate of compatibility rules previously suspended by the Commission due to implementation problems, and adopted an NPRM that proposed the rules recommended by the committee); National Primary Drinking Water Regulations: Monitoring Requirements for Public Drinking Water Supplies, 61 Fed. Reg. 24,354 (1996) (prior to adopting standards for the level of disinfection byproducts and pathogens in drinking water, the Environmental Protection Agency adopted an information collection requirement developed by a negotiated

rulemaking committee composed of state and local public health officials, local elected officials, consumer groups, water utilities and environmental groups).

Significantly, the Negotiated Rulemaking Act does not require agencies to use the formal procedures described above. *See* 5 U.S.C. § 561 ("Nothing in this subchapter should be construed as an attempt to limit innovation and experimentation with the negotiated rulemaking process or other innovative rulemaking procedures otherwise authorized by law."). More informal procedures may also be employed that do not require strict adherence to the Federal Advisory Committee Act. A recent example before the Federal Energy Regulatory Commission ("FERC") may provide a useful model for the Commission here. The FERC used an advanced notice of proposed rulemaking to initiate an informal negotiated rulemaking, asking industry participants to find areas of consensus for standards for electric power generation agreements. *See Standardization of Generator Interconnection Agreements and Procedures*, 67 Fed. Reg. 22,250 (May 2, 2002), 99 FERC ¶ 61,086 (2002). Public meetings, plenary sessions, private caucuses and drafting sessions produced consensus in a number of areas. The areas of consensus and the report provided to the agency by the participants formed the basis of the proposed rule issued by the agency. The proposal is now proceeding through a more typical notice-and-comment process, ensuring that all interested parties are able to participate.

Following this example, an informal negotiated rulemaking on DTV copy protection could seek the participation of affected industries, consumers and other interested parties in public meetings, plenary sessions, private caucuses and/or drafting sessions to attempt to reach a consensus on the unresolved issues identified by the Commission and the parties in this proceeding. Areas of consensus can form the basis of a proposed rule to be issued by the Commission, which will then proceed through the more typical notice-and-comment process.

Whether convened on a formal or informal basis, the negotiated rulemaking process will yield the most fruit if it adheres to a specific directive to consider:

- The effectiveness (including a cost-benefit analysis) and appropriateness of the broadcast flag technology proposed by certain commenters in this proceeding;
- The effectiveness (including a cost-benefit analysis) and appropriateness of source-encryption-based technologies;
- The standards that must be satisfied by any accepted technology or implementation method; and
- The interaction between the questions raised by the NPRM and digital copy protection for MVPD platforms.

V. CONCLUSION

For the foregoing reasons, Veridian urges the Commission not to adopt the broadcast flag proposal, but to conduct on an expedited basis a formal or informal negotiated rulemaking to determine whether and what DTV copy protection mandates are necessary.

Respectfully submitted,

/s/ Pantelis Michalopoulos

Paul B. Schneck
Vice President and Chief Technology Officer
Veridian Corporation
1200 South Hayes Street, Ste. 1100
Arlington, VA 22202
(703) 575-3100

Pantelis Michalopoulos
Rhonda M. Bolton
Steptoe & Johnson LLP
1330 Connecticut Avenue NW
Washington, DC 20036
(202) 429-3000

Counsel for Veridian Corporation

February 21, 2003